

**State of Montana Information Security Advisory Council**

**Minutes**

**January 11, 2017**

**1:00 PM**

**Cogswell Building, Room 151**

**Members Present:**

Ron Baldwin CIO/SITSD, Chair  
Erika Billiet, City of Kalispell  
Joe Frohlich, SITSD  
Stuart Fuller, DPHHS  
Kreh Germaine, DNRC

Jim Gietzen, OPI  
Lynne Pizzini, CISO/SITSD  
Dawn Temple, DOJ, Alternate  
Major General Matthew Quinn, DMA

**Staff Present:**

Wendy Jackson

**Guests Present:**

Eric Durkin, Rebecca Cooper, Lance Wetzel, Sean Rivera, Manuel Soto, Tom Murphy, Craig Stewart, Dave Johnson

**Real-time Communication:**

John Cross, Phillip English, Josh Gillespie, Josh Rutledge, Margaret Kauska, Jim Cosina, Jerry Marks, Terry Meagher, Sherry Mitschke, Daniel Nelson, Cheryl Pesta, Rawlin Richardson, Erin Stroop, Shannon Wells, Kyle Belcher

**Welcome and Introductions**

Ron Baldwin welcomed the council to the January 11, 2017 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

**Minutes**

**Motion:** Stuart Fuller made a motion to approve the November 17, 2016 minutes as presented. Dawn Temple seconded the motion. Motion carried.

Mr. Baldwin reported that there are changes to the council members. John Burrell is replacing Bryan Costigan and John Straughn is replacing John Daugherty. Both new council members were the designee of the previous council member.

Mr. Baldwin gave a report on the legislative session. State Information Technology Services Division (SITSD) reported to the General Government Appropriations Subcommittee on January 10, 2017. Lynne Pizzini gave a reported to the same subcommittee on the Cyber Security Posture and the MT-ISAC council.

Stuart Fuller reported that House Bill (HB)147 and HB 148 on privacy are fixed and the government has a special exemption not to acquire a subpoena to look at employee's personal devices.

**Business**

**Data Loss Prevention**

Joe Frohlich reviewed the history of Data Loss Prevention (DLP). A presentation regarding OneDrive for Business and SharePoint Online was given at MT-ISAC meeting in July 21, 2016. There have been regular updates to MT-ISAC and Information Technology Managers Council (ITMC) regarding the testing of DLP. In November, 2016, DLP was turned on in audit mode for state internal emails. The Montana driver's license has been removed from the template for now, do to many false positives. A case has been opened with Microsoft to address the driver's license. While audit mode has been in place, approximately 1600 emails per day are reporting state users sending sensitive information through email. The sender of the email will receive an alert regarding the error. SITSD is working to reduce the alert time.

Q: Dawn Temple: What if people mistake the alert for a phishing email?

A: Mr. Johnson: There is a form that is going to be sent out informing users of what DLP is and how it will

work.

**Action Item:** Jim Gietzen suggested that SITSD develop a communication template to notify users, and that he be able to edit it and send it out.

Mr. Johnson commented that when an email or attachment is flagged, an incident report is sent.

Q: Lynne Pizzini: Who gets the incident report?

A: Mr. Johnson: That will be determined.

Mr. Johnson reported that the external email settings are like internal settings and this option will be turned on in July, 2017.

Q: Ms. Temple: What about encrypted emails?

Mr. Baldwin commented that encrypted emails do not need to be read by DLP due to the encryption. However, all emails containing sensitive information should be encrypted. Also, DLP should block on one instance of sensitive information.

**Motion:** Lynne Pizzini made a motion to approve the template that SharePoint, OneDrive for Business and Exchange will block on one incident of sensitive information. Exchange will begin blocking after July 1, 2017.

Mr. Fuller seconded the motion. Motion carried.

**Motion:** Lynne Pizzini made a motion that SITSD will send a notification of an FAQ on DLP Friday, January 13, 2017. This will allow agencies two weeks to notify their staff of the implementation beginning January 28, 2017. Ms. Temple seconded the motion. Motion carried.

**Action Item:** Mr. Frohlich will add DLP to the MT-ISAC agenda as a standing item.

For more information regarding DLP, please contact Joe Frohlich at [JFrohlich@mt.gov](mailto:JFrohlich@mt.gov) or Dave Johnson at [Dave.Johnson@mt.gov](mailto:Dave.Johnson@mt.gov).

## **MT-ISAC Topics of Discussion**

### **Disposal of Media Storage – Destruction Process**

Mr. Frohlich reported on the disposal of media storage and how all destruction must be completed on site. All hard drives within the State of Montana Data Center are degaussed and given to Helena Industries for shredding.

### **Server Antivirus Update**

Mr. Frohlich reported that legal counsel has signed off on the contract regarding antivirus with Sophos. Notices will be sent out when the contract has been adopted so that Linux servers may be updated with Sophos.

### **EMET End of Life**

Mr. Frohlich reviewed the Enhanced Mitigation Experience Toolkit (EMET). The end of life for EMET is July 31, 2018. Microsoft and Gartner recommended migrating to the latest version of Windows 10. Microsoft Windows 7 users, as well as Windows 10 users can continue to use EMET after end of life, as it will provide an extra layer of protection for the devices.

Mr. Frohlich made a request to Brett Dahl, Division Administrator for the Risk Management and Tort Defense Division, to update Montana Code Annotated (MCA) 2-6-501. Once completed, Mr. Frohlich will update the MT-ISAC webpage found at <http://sitsd.mt.gov/Governance/ISAC>.

Mr. Frohlich reminded the council that agencies can save up to 55% on SANS Online Security Training if purchased before January 31, 2017. For more information, please contact Mr. Frohlich at [JFrohlich@mt.gov](mailto:JFrohlich@mt.gov).

Mr. Frohlich reported that Mr. Fuller suggested a presentation on the continuity of operations. In addition, he would like an update on the power incident that happened on November 17, 2016. Dawn Pizzini will update the council on these topics during the February 8, 2017 MT-ISAC meeting.

Lynne Pizzini reported that the State of Montana received an invitation to the National Governors Association "Meet the Threat" West Coast Summit in March, 2017. Major General Quinn and Lynne Pizzini are considering possible members to attend this event.

## **Workgroup Updates**

### **Assessment Workgroup**

## **Policy Assessment Tool Update – NCSR**

Mr. Frohlich gave a quick update on the Policy Assessment Tool. He sent an email to the council requesting if they would like to use the National Cyber Security Review (NCSR) document. Responses are due by close of business on January 13, 2017.

## **Best Practices / Tools Workgroup Update**

### **Acceptable Use – Rules of Behavior**

Lynne Pizzini reported that the best practices workgroup continues to incorporate the requested changes to the Acceptable Use – Rules of Behavior best practices document from the MT-ISAC October 27, 2016 meeting. The updated document will be posted to the MT-ISAC website (<http://sitsd.mt.gov/Governance/ISAC>) within a few weeks. At which time, Mr. Frohlich will email the council when it is ready for review.

**Action Item:** Joe Frohlich will add the Acceptable Use – Rules of Behavior best practices document as an action item on the February 8, 2017 MT-ISAC meeting.

### **Identification and Authentication**

Mr. Frohlich reported that the Identification and Authentication document has been placed on the MT-ISAC website at <http://sitsd.mt.gov/Governance/ISAC>. Any comments can be sent to Joe Frohlich at [JFrohlich@mt.gov](mailto:JFrohlich@mt.gov).

**Action Item:** Joe Frohlich will add Identification and Authentication as an action item on the February 8, 2017 MT-ISAC meeting.

### **AV Augmentation**

Mr. Frohlich gave an update regarding AV Augmentation. The best practices workgroup approved the Microsoft Endpoint Protection as State of Montana antivirus. Gartner was sent a list of requirements regarding augmentation of the antivirus.

### **Situational Awareness / Outreach / Public Safety Workgroup Update**

Mr. Frohlich reported that the Department of Justice (DOJ) provided the Situational Workgroup some toolkits which contain contact information for associations around the State of Montana. These toolkits will be helpful during outreach to these associations.

### **Current Threats**

Sean Rivera reported that a new campaign is targeting Human Resource (HR) departments through job applications. HR employees receive an email containing a PDF Cover Letter and an Excel Spreadsheet with GoldenEye Ransomware.

Mr. Rivera also reported for the year 2016 SITSD tripled the amount of attachments that were blocked compared to the last five or six years. SITSD had 29B denied Firewall Packets compared to 12.6B in prior years.

### **Open Forum**

#### **Future Agenda Items**

**Action Item:** Mr. Germaine requested the NCSR process documentation addressed at the next MT-ISAC meeting.

### **Public Comment**

Rebecca Cooper, Fish Wildlife & Parks (FWP), requested more information regarding the immediate destruction topic. FWP would like to work with other agencies to combine efforts due to the small amount of shredding FWP requires.

**Action Item:** Joe Frohlich and Lynne Pizzini will investigate an Enterprise Solution for Destruction of Media Storage.

Ms. Cooper also asked if the DLP presentation was available online.

**Action Item:** CIO Support will post the Data Loss Prevention presentation to the MT-ISAC website <http://sitsd.mt.gov/Governance/ISAC>.

### **Next Meeting**

February 8, 2017  
1:00 PM to 3:00 PM  
Cogswell Building, Room 151

**Adjournment**

The meeting adjourned at 2:55 PM.